

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

TINA CLAYTON, individually and on
behalf of others similarly situated,

Plaintiff,

v.

PRUITTHEALTH, INC.,

Defendant.

CIVIL ACTION FILE
NO. 1:24-CV-2960-TWT

OPINION AND ORDER

This is a data breach case. It is before the Court on Defendant PruittHealth, Inc.’s (“PruittHealth”) Motion to Dismiss [Doc. 24]. For the reasons set forth below, PruittHealth’s Motion to Dismiss [Doc. 24] is GRANTED in part and DENIED in part.

I. Background¹

Plaintiff Tina Clayton was employed by Defendant PruittHealth from approximately 2000 through 2010. (Am. Compl. [Doc. 22] ¶ 17.) As a healthcare provider, PruittHealth collects certain information from its employees and patients. (*Id.* ¶ 31.) In November 2023, cybercriminals hacked into PruittHealth’s systems and acquired copies of electronic files containing the sensitive information of at least 56,405 employees and patients. (*Id.* ¶¶ 1–

¹ The Court accepts the facts as alleged in the Amended Complaint as true for purposes of the present Motion to Dismiss. *Wilding v. DNC Servs. Corp.*, 941 F.3d 1116, 1122 (11th Cir. 2019).
T:\ORDERS\24\Clayton\24cv2960\mtdtw.docx

3; *id.* ¶ 37 (citing *Notice of Data Security Incident*, PruittHealth, <https://www.pruitthealth.com/cybersecurity-breach-notice> (last visited June 6, 2025)).) The hackers threatened to publish the files on a “dark web” blog site unless PruittHealth paid a ransom, (*id.* ¶ 37), which PruittHealth presumably did not do. In December 2023, the hackers claimed that they published the files on the dark web site, but PruittHealth’s forensic specialists could not verify this fact because the site “was taken down” by the time they tried to access the files. (*Id.*) According to the notice that Clayton received, the exposed information potentially includes her (and others’) “full or partial name, date of birth, government identification information, demographic information, contact information, home address, financial information including, Social security numbers, bank account number, health insurance information, and health information.” (*Id.*) On behalf of herself and a putative class, Clayton seeks relief on three counts: (1) negligence, (2) negligence per se, and (3) breach of fiduciary duty. PruittHealth presently moves to dismiss the Amended Complaint under Rule 12(b)(6).

II. Legal Standard

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a “plausible” claim for relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); Fed. R. Civ. P. 12(b)(6). A complaint may survive a motion to dismiss for failure to state a claim, however, even if it is

“improbable” that a plaintiff would be able to prove those facts and even if the possibility of recovery is extremely “remote and unlikely.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007). In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff. *See Quality Foods de Centro Am., S.A. v. Latin Am. Agribusiness Dev. Corp.*, 711 F.2d 989, 994–95 (11th Cir. 1983); *see also Sanjuan v. Am. Bd. of Psychiatry & Neurology, Inc.*, 40 F.3d 247, 251 (7th Cir. 1994) (noting that, at the pleading stage, the plaintiff “receives the benefit of imagination”). Generally, notice pleading is all that is required for a valid complaint. *See Lombard’s, Inc. v. Prince Mfg., Inc.*, 753 F.2d 974, 975 (11th Cir. 1985). Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff’s claim and the grounds upon which it rests. *See Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (citing *Twombly*, 550 U.S. at 555).

III. Discussion²

A. Failure to Allege Any Injury (All Counts)

Clayton must establish a cognizable injury for all three of her tort claims. *See Collins v. Athens Orthopedic Clinic, P.A.*, 307 Ga. 555, 557–58

² Regarding all three of Clayton’s tort claims, both parties agree that the Court must apply Georgia substantive law for the purposes of this Motion to Dismiss. (Br. in Supp. of Def.’s Mot. to Dismiss, at 6; see Pl.’s Resp. Br. in Opp’n to Def.’s Mot. to Dismiss, at 3–13.)

(2019). While actual identify theft, fraud, and their associated damages most clearly can constitute cognizable injuries, a plaintiff can also establish a cognizable injury by showing a substantial and imminent risk of theft and fraud. *Tracy v. Elekta, Inc.*, 667 F. Supp. 3d 1276, 1283 (N.D. Ga. 2023). The alleged injury cannot be too speculative or remote, however. *Collins*, 307 Ga. at 558. At the motion-to-dismiss stage, Clayton must allege a cognizable injury with plausibility. *Twombly*, 550 U.S. at 557 (2007).

PruittHealth seeks to dismiss the Amended Complaint for failure to plausibly allege a cognizable injury for any of its three tort claims. Specifically, PruittHealth argues that the Amended Complaint fails to allege that (1) Clayton’s personal data “was actually sold or published on the dark web” or (2) Clayton became the “victim of identify theft or fraud” due to the data breach. (Br. in Supp. of Def.’s Mot. to Dismiss, at 7 [Doc. 24-1].)

The Court holds that Clayton plausibly pleads a cognizable injury as to all three of her tort claims. While Clayton has not been the victim of any actual identify theft or other misuse of her data (to date), she alleges that the data breach has created a substantial and imminent risk of identity theft and fraud. (*See, e.g.*, Am. Compl. ¶¶ 11, 102, 105.) She also alleges injuries such as loss of privacy, loss of value of her private information, loss of time from monitoring her accounts and financial records, emotional distress, and anxiety. (*Id.* ¶¶ 101, 107, 110–112). Additionally, Clayton alleges that she may incur in the

future certain out-of-pocket expenses associated with credit monitoring services and other services aimed toward protecting her identity and accounts. (*Id.* ¶¶ 12, 106.)

The Georgia Supreme Court considered similar facts in *Collins v. Athens Orthopedic Clinic, P.A.*, 307 Ga. 555 (2019), and held that the data breach victims there sufficiently pleaded a cognizable injury. *Id.* at 563–64 (“[The Plaintiffs’] allegation that the criminal theft of their personal data has left them at an imminent and substantial risk of identity theft is sufficient at this stage . . .”). In *Collins*, the Georgia Supreme Court presumed as true the allegations that a criminal actor maliciously “stole a large amount of personal data” (including social security numbers, address, birth dates), the criminal actor “attempted to sell at least some of [it],” and criminals had the “ability to use the stolen data” for identity theft and fraud.³ *Id.* at 562. The Court there

³ The Court notes that at least three federal district courts have interpreted *Collins* and held that plaintiffs have plausibly pleaded cognizable injuries with lesser allegations, though the Court does not rely on their reasonings in the instant case. *Tracy*, 667 F. Supp. 3d at 1282–83 (finding a cognizable injury despite no allegations that the data may have been published or sold); *Teague v. AGC Am., Inc.*, 2025 WL 1527738, at *5 (N.D. Ga. Jan. 6, 2025) (same); *Bracy v. Americold Logistics LLC*, 2025 WL 552676, at *4 (N.D. Ga. Feb. 19, 2025) (same). As Clayton points out, the Eleventh Circuit has also noted in dicta that *Collins* “recognized a cognizable injury where a criminal theft of the plaintiffs’ personal data allegedly put them at an imminent and substantial risk of identity theft.” *Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1218 (11th Cir. 2023). These cases appear to leave open the possibility that future plaintiffs may establish an injury by merely pointing to a large data breach by a criminal actor, but I do not go that far in ruling on the pending motion.

found that these allegations “raise[d] more than a mere specter of harm,” *id.* at 563, and that it was not too far a leap to infer that “the plaintiffs [] likely will suffer identity theft,” *id.* at 562. Particularly significant to the Court was the fact that the data breach occurred as a result of criminal hackers. *Id.* It explained that “showing injury as a result of the exposure of data is easier . . . where the data exposure occurs as a result of an act by a criminal whose likely motivation is to sell the data to others.” *Id.* Additionally, the Court noted that its conclusion did not depend on whether any named plaintiffs had actually experienced identity theft. *Id.* at 564, n.8.

This Court reaches the same conclusion as the Georgia Supreme Court in *Collins*.⁴ Clayton alleges that cybercriminals hacked into PruittHealth’s systems and made copies of files with sensitive data such as full names, addresses, birth dates, social security numbers, and banking information. (Am. Compl. ¶ 37.) As with the plaintiff in *Collins*, Clayton alleges that hackers accessed sensitive information of the exact kind that is commonly used for fraud and identity theft and did so on a mass scale. (*Id.* ¶¶ 1–3, 72–73.) Moreover, construing the facts in the light most favorable to the Plaintiff, the Court finds it plausible that Clayton’s personal information was published on the dark web. PruittHealth itself acknowledged in its data breach notice that

⁴ Although the Court finds *Collins* persuasive and applies its underlying reasoning accordingly, the Court acknowledges that *Collins* applied Georgia’s pleading standards rather than federal pleading standards, as is required here.

the hackers stated they published the files on their dark web blog site. (*Id.* ¶ 100.) Although PruittHealth’s forensic specialists were unable to confirm this fact because the blog site “was taken down” at the time of their review, (*id.* ¶ 37), the hackers’ claim itself is sufficient to allow a reasonable inference that the files were published at some point and thus made available for further criminal use.⁵ These allegations taken together plausibly speak to the substantial and imminent risk of theft and fraud—a cognizable injury—despite the lack of any allegations of actual theft or fraud. And, having found a risk of theft and fraud, the Court need not dismiss Clayton’s additional damages theories (e.g., loss of time to monitor accounts, loss of privacy) at this stage.

B. Negligence (Count I)

To establish a claim for negligence in Georgia, a plaintiff must establish the existence of a legal duty, a breach of that duty, causation, and damages. *Collins*, 307 Ga. at 557. According to PruittHealth, the Amended Complaint fails to allege any duty or causation. (Br. in Supp. of Def.’s Mot. to Dismiss, at 12.) The Court discusses causation first, followed by duty.

First, the Court finds that Clayton plausibly pleads causation. The

⁵ The Court also notes that it is unclear how much time had passed between the hackers’ claim that the files were published and PruittHealth’s attempt to review the files. Without this information and drawing all inferences in favor of Clayton, the Court is further comfortable finding that it was plausible that the files were in fact published at some point and before PruittHealth’s forensic specialists could review them.

Court has already found that Clayton faces an imminent and substantial risk of identity theft and fraud due to the data breach. (Am. Compl. ¶¶ 2–3.) The Amended Complaint alleges that the data breach was proximately caused by PruittHealth’s failure to adequately secure and monitor its systems. (*Id.* ¶ 139 (listing eight ways in which PruittHealth failed to do so).) It also specifically alleges that PruittHealth failed to comply with industry standards regarding cybersecurity. (*Id.* ¶ 59 (alleging that PruittHealth failed to comply with the “NIST Cybersecurity Framework Version 1.1” and “Center for Internet Security’s Critical Security Controls”).) Taking these allegations as true, the Court finds causation adequately pleaded—and especially so given that the innerworkings and history of a company’s security systems are often not available without discovery. *See Ramirez v. Paradise Shops, LLC*, 69 F.4th 1213, 1220–21 (11th Cir. 2023).

Second, the Court finds that Clayton plausibly pleads the existence of a duty. According to PruittHealth, the Georgia Supreme Court held in *Department of Labor v. McConnell*, 305 Ga. 812 (2019), that no common law duty to safeguard personal information exists. (Br. in Supp. of Def.’s Mot. to Dismiss, at 13 (quoting *McConnell*, 345 Ga. App. at 798–99).) The Court disagrees and finds that *McConnell* does not stand for such a broad proposition. In *McConnell*, a Department of Labor employee sent out a mass email that inadvertently contained the sensitive information (e.g., names, social security

numbers) of thousands of Georgia residents. 305 Ga. at 812–13. The plaintiff argued that the Department of Labor owed him a duty to protect his personal information, arising from a “general legal duty ‘to all the world not to subject [others] to an unreasonable risk of harm.’” *McConnell*, 305 Ga. at 815–16 (alteration in original) (quoting *Bradley Center, Inc. v. Wessner*, 250 Ga. 199, 201 (1982)). The Georgia Supreme Court, however, rejected the idea that any such general legal duty to all exists and upheld the dismissal of the plaintiff’s negligence claim for failure to establish any other basis for a duty to protect personal information. *Id.* at 816 (finding that a duty to protect personal information did not arise under O.C.G.A. §§ 10-1-393.8, 10-1-910 either).

Notably, *McConnell* did not altogether reject the existence of a duty to safeguard personal information; rather, it only rejected certain bases for such a duty. Other courts appear to agree. For example, the Georgia Supreme Court in *Collins* declined to address the duty issue but described *McConnell* as holding that “[the] plaintiff failed to show that [a] state agency owed him [a] duty—under either O.C.G.A. § 10-1-393.7, O.C.G.A. § 10-1-910, or [a] purported common law duty ‘to all the world . . .’—to protect their personal information from inadvertent, negligent disclosure.” *Collins*, 307 Ga. at 316 (emphasis added). In *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360 (N.D. Ga. 2021), this district reviewed *McConnell* and *Collins* and concluded that *McConnell* left open the possibility that other circumstances may give rise

to a duty to protect personal information. *Id.* at 1368 (“[I]f *McConnell* had already answered the question as to whether such a duty could arise under Georgia law, th[e] discussion in *Collins* (and indeed the court’s holding) would make little sense.”); *see also Tracy*, 667 F. Supp. 3d at 1284 (“*Collins* . . . certainly did not foreclose the existence of a duty to protect personal information.”).

Here, the Court finds that Clayton plausibly alleges that PruittHealth had a legal duty to protect her personal information, at least on the basis of the foreseeable risk of a data breach in this instance. The Eleventh Circuit held in *Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213 (11th Cir. 2023), that a defendant employer owed a legal duty to its employees to protect their personal information from a data breach, given the plaintiff’s plausible allegations that the risk of a data breach was reasonably foreseeable. *Id.* at 1220–21. The Eleventh Circuit based its finding on Georgia’s traditional tort law principles: A defendant has “no duty to rescue another from a situation of peril which the former has not caused,” but a relationship may arise that “imposes a duty” to render assistance if a “defendant’s own negligence has been responsible for the plaintiff’s situation.” *Id.* at 1219 (emphasis omitted) (quoting *City of Douglasville v. Queen*, 270 Ga. 770, 773 (1999) and *Thomas v. Williams*, 105 Ga. App. 321, 326 (1962)); *see also id.* (“[T]he creator of a potentially dangerous situation has a duty to eliminate the danger or give warning to others of its

presence.” (quoting *City of Winder v. Girone*, 265 Ga. 723, 724 (1995))). But the scope of the duty must typically be “limited to reasonably foreseeable risks of harm.” *Id.* (quoting *Maynard v. Snapchat, Inc.*, 313 Ga. 533, 537 n.3 (2022)). Applying these principles at the motion-to-dismiss stage, the Eleventh Circuit determined that the defendant company in *Ramirez* inadequately protected its employees’ sensitive data, creating a danger of a data breach that the defendant had a duty to address. *See id.* at 1220.

The same principles and kind of allegations are present here. Like the plaintiff in *Ramirez*, Clayton plausibly pleads that her employer had a legal duty to protect her personal information from the reasonably foreseeable danger of a data breach. (Am. Compl. ¶¶ 140, 132.) She pleads that PruittHealth was her employer and required her to provide certain sensitive data “as a condition of her employment,” (*id.* ¶ 18), but that PruittHealth inadequately protected such information, (*id.* ¶ 7). Moreover, PruittHealth was allegedly aware of the danger of a data breach “[b]ecause it was widely known and reported that healthcare providers are a frequent target of data thieves.” (*Id.* ¶ 131; *see also id.* ¶ 140 (noting the “known high frequency of cyberattacks and data breaches in the healthcare industry”); *id.* ¶¶ 85–86, 140 (regarding the high value of medical data and the disproportionately high number of healthcare-related data breaches)). These allegations go beyond those considered in *Ramirez*, where the Eleventh Court “dr[ew] on [its] judicial

experience and common sense” to “reasonably infer” that a company of the defendant’s “size and sophistication” and with “such an extensive database of prior employees’ [personally identifiable information]” should have “foreseen being the target of a cyberattack.” *Ramirez*, 69 F.4th at 1220. Therefore, the Court declines to dismiss the negligence claim for failure to establish a duty.

C. Negligence per Se (Count II)

To establish a claim for negligence per se in Georgia, a plaintiff must establish that “a statute is violated, the person injured by the violation is within the class of persons the statute was intended to protect, and the harm complained of was the harm the statute was intended to guard against.” *Murphy v. Bajjani*, 282 Ga. 197, 200 (2007) (citation omitted).

Clayton cites the Health Insurance Portability and Accountability Act (HIPAA) and § 5 of the Federal Trade Commission Act (FTCA) to support her claim for negligence per se. Specifically, she argues that PruittHealth failed to meet (1) HIPAA regulations, pursuant to 42 U.S.C. 15 U.S.C. § 1301 *et seq.*, regarding the protection of confidential health information, (Am. Compl. ¶¶ 61–65), and (2) FTCA regulations, pursuant to 15 U.S.C. § 45, regarding the protection of confidential consumer data, (*id.* ¶¶ 48–55).

The Court dismisses the negligence per se claim as to both HIPAA and the FTCA. First, the Court agrees with PruittHealth that negligence per se claim must be dismissed to the extent it concerns HIPAA since Clayton has not

plausibly pleaded that any of her health information was exposed. (Reply Br. in Supp. of Def.'s Mot. to Dismiss, [Doc. 26], at 11.) Clayton was an employee of PruittHealth but never a patient, and the Amended Complaint does not explain how Clayton's protected health information might have ever been collected by PruittHealth.

Second, the Court dismisses the negligence per se claim as to the FTCA for failure to establish that Clayton is within the class of persons that the FTCA was intended to protect. As an initial matter, the Court agrees with Clayton that the FTCA *can* be the basis for a negligence per se claim involving a data breach. *See Tracy*, 667 F. Supp. 3d at 1285 (collecting cases); *see also id.* ("Section 5 can provide the basis of a negligence per se claim regardless of whether the statute itself supplies a private right of action."); *Briggs v. N. Highland Co.*, 2024 WL 519722, at *9 (N.D. Ga. Feb. 9, 2024) ("After review, the Court continues to align with other decisions from this district that conclude that negligence *per se* in Georgia applies to the FTCA."). This is notwithstanding PruittHealth's arguments to the contrary. (Br. in Supp. of Def.'s Mot. to Dismiss, at 19 (arguing that the FTCA cannot support a negligence per se claim because there is no private right of action and because it does not outline any duties, standards, or substantive requirements).)

That being said, the Court is persuaded by independent grounds to dismiss the negligence per se claim as to the FTCA. As this Court recently held

in *Bracy v. Americold Logistics LLC*, 2025 WL 552676 (N.D. Ga. Feb. 19, 2025), an employee whose information was exposed in a data breach cannot state a claim for negligence per se under § 5 of the FTCA because that section was intended to protect only “consumers” and “competitors.” *Id.* at *5. The Court provided the following basis:

Section 5 of the FTC Act states, “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.” 15 U.S.C. § 45(a)(1). It further specifies that the FTC “shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C. § 45(n). “Congress, through [Section] 5, charged the FTC with protecting consumers as well as competitors.” *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 (1972); *see also FTC v. Raladam Co.*, 283 U.S. 643, 647–48 (1931) (“The paramount aim of the act is the protection of the public from the evils likely to result from the destruction of competition or the restriction of it in a substantial degree.”).

Id. It further relied on decisions in other courts that limited the class of § 5 of the FTCA to consumers and competitors. *Id.* (collecting cases, and distinguishing other cases handed down prior to *Loper Bright Enterprises v. Raimondo*, 603 U.S. 369, 412 (2024)). *But see Briggs*, 2024 WL 519722, at *1, 9 (denying dismissal of a plaintiff employee’s FTCA-based negligence per se claim, but without an analysis on the employee-versus-consumer issue). The reasoning in *Bracy* applies here: Clayton alleges she was PruittHealth’s employee—not its consumer or competitor—and thus she is not within the

class of persons that § 5 of the FTCA was intended to protect. The Court accordingly dismisses the negligence per se claim as to the FTCA.

D. Breach of Fiduciary Duty (Count III)

To establish a claim for breach of fiduciary duty in Georgia, a plaintiff must establish “(1) the existence of a fiduciary duty; (2) breach of that duty; and (3) damage proximately caused by the breach.” *UWork.com, Inc. v. Paragon Techs., Inc.*, 321 Ga. App. 584, 594 (2013) (citation omitted). A fiduciary duty exists “where one party is so situated as to exercise a controlling influence over the will, conduct, and interest of another or where, from a similar relationship of mutual confidence, the law requires the utmost good faith.” *Bedsole v. Action Outdoor Advert. JV, LLC*, 325 Ga. App. 194, 201 (2013) (quoting O.C.G.A. § 23-2-58).


The Court holds that, although PruittHealth employed Clayton, it did not owe her a fiduciary duty. The Georgia Supreme Court has stated that “[t]he employee-employer relationship is not one from which the law will necessarily imply fiduciary obligations.” *Atlanta Mkt. Ctr. Mgmt., Co. v. McLane*, 269 Ga. 604, 607 (1998). While it is also true that “the facts of a particular case may establish the existence of” an employee-employer fiduciary relationship, *id.*, the facts here do not establish the existence of such a relationship. Clayton argues that PruittHealth owed her a fiduciary duty because she was in “a poor position to protect . . . her own interests” regarding “the collection and

retention of highly sensitive employee data” and the possibility of “grievous harm if handled badly.” (Pl.’s Resp. Br. in Opp’n to Def.’s Mot. to Dismiss, [Doc. 25], at 12–13 (analogizing this case to a line of cases in which Georgia courts have held that employers owe their employees a fiduciary duty “when selecting employee insurance plans, making changes to the plans, and representing the insurance to employees”).) But obtaining certain sensitive information such as names, addresses, dates of birth, social security numbers, and banking information is “common practice for almost any form of employment.” *Purvis*, 563 F. Supp. 3d at 1384. Providing such information does not create a fiduciary relationship or suggest that Clayton was “relying upon or trusting [PruittHealth] in unique or exceptional ways” *Id.* Therefore, the Court grants PruittHealth’s Motion to Dismiss Count III (breach of fiduciary duty).

IV. Conclusion

For the reasons set forth above, PruittHealth’s Motion to Dismiss [Doc. 24] is GRANTED as to Counts II and III, and it is DENIED as to Count I.

SO ORDERED, this 9th day of June, 2025.


THOMAS W. THRASH, JR.
United States District Judge